ETHME – Status Update III

ETHME time & task recording			
project workload	125,00 h	team size	1 persons
per person	125,00 h		
		start	23.9.2019
workload left over	58,50 h	end	28.10.2019
per person	58,50 h	duration	5 weeks
left h per week / person	**27,30 h**	today	13.10.2019
per working day	**5,46 h**	till end	**2 weeks**
Projects GitHub:	https://github.com/arminbrandy/ethme	total	**66,50 h**

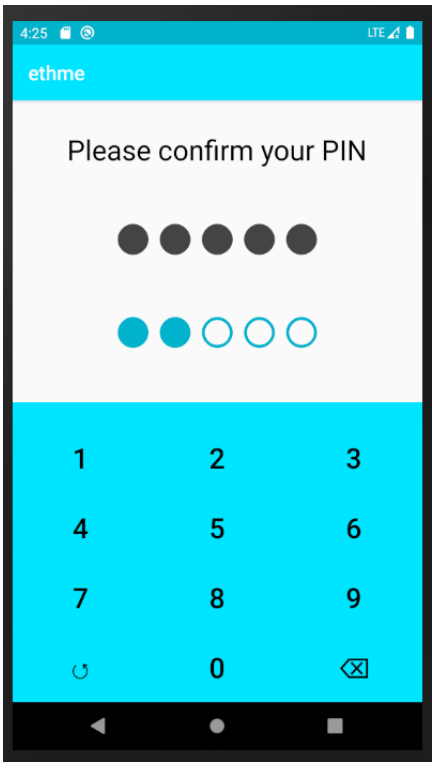
Armin Brandy		
task - *commit*	**hours**	**date**
Research & evaluation	4,00 h	23.09.2019
Defining and writing the Vision as "Whitepaper" - *look at init commit - *ebbcc22*	2,00 h	23.09.2019
Start reading Mastering Ethereum	3,00 h	26.09.2019
Setup Project, basic environment & GitHub	3,00 h	27.09.2019
FH Blockchain LV - more about blockchain	3,00 h	27.09.2019
Starting Project, more environment & creating basic App - *4b636ea*	4,00 h	28.09.2019
ETHME - Status Update I	1,25 h	28.09.2019
Working on connecting to node via web3j and on Wallet creation...	4,50 h	29.09.2019
Successfully testing first web3j Wallet functionalities with web3j doc	4,50 h	02.10.2019
Learning about Wallet standards as BIP39/44 and related, Javas 'true' SecureRandom fns Exploring & testing wallet creation & storage with web3j and understanding the concepts	7,50 h	03.10.2019
Concept of user auth to access wallet & PIN activity for user authentication	2,75 h	04.10.2019
FH Blockchain LV - more into Ethereum & smart contracts	3,25 h	04.10.2019
Design PIN activity & designing secure storage structure	4,00 h	05.10.2019
ETHME - Status Update II	1,50 h	05.10.2019
Some redesign, PinPad activity & exact wallet encryption concept via PIN & Fingerprint	7,25 h	08.10.2019
Defined user & data flow of whole wallet creation process	4,25 h	10.10.2019
Finishing PinPad setup functionality - *4af0a1d*	5,25 h	11.10.2019
ETHME - Status Update III	1,50 h	11.10.2019

Progress

Since we now have already learned a lot about the different components of that project the next task was to create a detailed concept of how they should work together to enable a secure wallet creation & storage process. This task has been solved now and we have a concrete concept of how to implement the wallet file encryption and also how the user & data should flow during this process.

Furthermore the PinPad module, which has been a soley template the last time. Now has fully and clean implemented functionality for the PIN creation.
Using it for the PIN request and for a potential PIN change will be a task for later, since it's not relevant for the current wallet creation functionality. Either way, it shouldn't be that much of a work to adapt the current module to those functionalities later on.

Except of those bigger tasks, also some little redesign and code refactoring was done in this week.



Basic concept of encrypted wallet file storing

1. Ask User for a new PIN using the PinPad module
2. Using this PIN in combination with an, application restricted, asymmetric key provided by Androids Keystore module and let this new PIN be signed by the keypairs private key, which is securely stored by the Android OS itself.
3. This gives us a unique, long and deterministic String/Byte array, which is only reproduceable knowing the PIN and having access to the devices KeyStore, which solely the application itself has.
4. We now use this data as password to encrypt the actual new created Wallet file, without the need of either storing the PIN, nor this password of the Wallet file. Which meets the wished requirements of having stored only the Wallet file with a strong not easy to brute force password.

a) If we later on want to add the fingerprint functionality, we'll also use Android Keystore in combination with a key which is only accessible after the User authenticated itself using his fingerprint.

b) With this different key we'll encrypt the rare PIN and store this encrypted file next to the encrypted wallet file.

c) If a user now wants to access his wallet using his fingerprint, the fingerprint will unlock the key, which lets us decrypt the encrypted PIN and then use this PIN again as it is described in the normal PIN verification.

How are we proceeding

In the last Status update I mentioned the tight timeframe for that project. Now in cooperation with the Tutor, a new deadline was agreed.
Which will be Monday the 28. Oct 2019

Next task is implementing the developed concept and user flow for the wallet creation and then continue with basic wallet operations, as displaying the accounts eth balance, address and also be able to send a basic eth transaction.